

THE SOLUTION TO THE KADISON–SINGER PROBLEM: YET ANOTHER PRESENTATION

DAN TIMOTIN

ABSTRACT. In the summer of 2013 Marcus, Spielman, and Srivastava gave a surprising and beautiful solution to the Kadison–Singer problem. The current presentation is slightly more didactical than other versions that have appeared since; it hopes to contribute to a thorough understanding of this amazing proof.

CONTENTS

1. Introduction	2
2. The Kadison–Singer problem	2
2.1. Pure states	2
2.2. The Kadison–Singer conjecture	3
2.3. The Paving Conjecture	4
3. Intermezzo: what we will do next and why	6
3.1. General plan	6
3.2. Sketch of the proof	6
4. Analytic functions and univariate polynomials	7
4.1. Preliminaries	7
4.2. Nice families	9
5. Several variables: real stable polynomials	10
5.1. General facts	10
5.2. The barrier function	12
6. Characteristic and mixed characteristic polynomials	15
6.1. Mixed characteristic polynomial	15
6.2. Decomposing in rank one matrices and the characteristic polynomial	17
7. Randomisation	18
7.1. Random matrices and determinants	18
7.2. Probability and partitions	20
8. Proof of the Paving Conjecture	21
9. Final Remarks	23
References	24

1. INTRODUCTION

The Kadison–Singer Problem has been posed in [7] in the fifties, probably in relation to a statement of Dirac concerning the foundations of quantum mechanics. It has soon acquired a life of its own. On one hand, there have been several notable attempts to prove it. On the other hand, it has been shown that it is equivalent to various problems in Hilbert space theory, frame theory, geometry of Banach spaces, etc. However, for five decades the problem has remained unsolved.

It is therefore very remarkable that in 2013 a proof has been given by Marcus, Spielman and Srivastava in [10]. The methods used were rather unexpected; moreover, they had shown their strength in some totally unrelated areas (Ramanujan graphs). They also have a very elementary flavour: most of the proof is based on a delicate analysis of the behavior of polynomials in one or several variables.

In the year and a half that has passed a better grasp of the proof has been achieved, most notably through Terence Tao’s entry in his blog [14] (but see also [11]). It still remains an astonishing piece of research, obtaining spectacular results on a long standing conjecture through some not very complicated and apparently unrelated arguments.

The purpose of these notes is to contribute towards a better understanding of the MSS proof. There is of course no pretense to any originality: the content is essentially in [10], with some supplementary simplification due to [14] (and occasionally to [15]). But we have tried to make it more easy to follow by separating clearly the different steps and emphasizing the main arguments; also, in various places we have gone into more details than in the other presentations. It is to be expected that the methods of [10] might lead to new fruitful applications, and so it seemed worth to analyze them in detail.

It is clear from the above that the notes concentrate on the MMS proof, so there will be very little about the Kadison–Singer problem itself and about the plethora of research that had evolved in the last fifty years on its relations to other domains. In particular, with one exception that we need to use (the paving conjecture), we will not discuss the different reformulations and equivalent statements that have been obtained. For all these matters, one may consult former beautiful presentations, as for instance [4].

We will give in the next section a brief presentation of the original problem, as well as of another assertion, the paving conjecture, which has been shown soon afterwards to imply it. The description of the remaining part of the paper is postponed to Section 3, where the reader will have a general overview of the development of the proof.

These notes have been written for a series of lectures given in December 2014 at the Indian Statistical Institute in Bangalore, in the framework of the meeting *Recent Advances in Operator Theory and Operator Algebras*. We thank B.V.R. Bath, J. Sarkar, and V.S. Sunder for the excellent work done in organizing the workshop and the conference, as well as for the invitation to present the lectures.

2. THE KADISON–SINGER PROBLEM

2.1. Pure states. The material in this subsection is contained in standard books on C^* -algebras (see, for instance, [6]).

We denote by $B(\mathcal{H})$ the algebra of all bounded linear operators on the Hilbert space \mathcal{H} . A C^* -algebra $\mathcal{A} \subset B(\mathcal{H})$ is a norm closed subalgebra of $B(\mathcal{H})$, closed to the operation of taking the adjoint, and containing the identity.

A *state* on a C^* -algebra \mathcal{A} is a linear continuous map $\phi : \mathcal{A} \rightarrow \mathbb{C}$, which is positive (meaning that $\phi(a^*a) \geq 0$ for any $a \in \mathcal{A}$), and such that $\phi(I) = 1$. One proves then that $\|\phi\| = 1$ and that ϕ satisfies the *Cauchy-Schwarz* inequality

$$(2.1) \quad |\phi(b^*a)|^2 \leq \phi(a^*a)\phi(b^*b)$$

for all $a, b \in \mathcal{A}$.

The set $\mathfrak{S}(\mathcal{A})$ of all states on \mathcal{A} is a convex, w^* -compact subset of \mathcal{A}^* . A state ϕ is called *pure* if it is an extreme point of $\mathfrak{S}(\mathcal{A})$.

Example 2.1. If \mathcal{A} is commutative, then by Gelfand's Theorem it is isomorphic to $C(X)$, the algebra of continuous functions on the compact space X of all *characters* (multiplicative homomorphisms) $\chi : \mathcal{A} \rightarrow \mathbb{C}$. The dual $C(X)^*$ is formed by all Borel measures on X , and $\mathfrak{S}(C(X))$ is the set of probability measures on X . Pure states are precisely Dirac measures. In particular (and this is a fact that we will use below) a pure state on a commutative C^* -algebra is multiplicative.

Example 2.2. If $\mathcal{A} = B(\mathcal{H})$, $\xi \in \mathcal{H}$, and $\|\xi\| = 1$, then one can prove that $\phi_\xi(T) := \langle T\xi, \xi \rangle$ is a pure state. This fact will not be used in the sequel.

By a theorem of Krein (see, for instance, [12, Ch.I.10]) any state ϕ on a C^* -algebra \mathcal{A} extends to a state $\tilde{\phi}$ on $B(\mathcal{H})$. The set K_ϕ of all extensions of ϕ is a convex w^* -compact subset of $B(\mathcal{H})^*$.

Lemma 2.3. *If ϕ is a pure state on $\mathcal{A} \subset B(\mathcal{H})$, then the extreme points of K_ϕ are pure states of $B(\mathcal{H})$.*

Proof. Suppose ϕ is an extreme point of K_ϕ . If $\tilde{\phi} = \frac{1}{2}(\psi_1 + \psi_2)$, with ψ_1, ψ_2 states on $B(\mathcal{H})$, then $\phi = \frac{1}{2}(\psi_1|_{\mathcal{A}} + \psi_2|_{\mathcal{A}})$. Since ϕ is pure, we must have $\psi_1|_{\mathcal{A}} = \psi_2|_{\mathcal{A}} = \phi$, so $\psi_1, \psi_2 \in K_\phi$, and therefore $\psi_1 = \psi_2 = \phi$. \square

Consequently, a pure state ϕ on \mathcal{A} has a unique extension to a state on $B(\mathcal{H})$ if and only if it has a unique *pure* extension to a state on $B(\mathcal{H})$.

2.2. The Kadison-Singer conjecture. From now on we will suppose that the Hilbert space \mathcal{H} is $\ell^2 = \ell^2(\mathbb{N})$ and we will consider matrix representations of operators on $B(\ell^2)$ with respect to the usual canonical basis of ℓ^2 . We define \mathcal{D} to be the C^* -algebra of operators on ℓ^2 whose matrix is diagonal. Note that the map $\text{diag} : B(\ell^2) \rightarrow \mathcal{D}$ which sends an operator T to the diagonal operator having the same diagonal entries is continuous, positive, of norm 1.

We may now state the *Kadison-Singer Problem*:

Does any pure state on \mathcal{D} extend uniquely to a state on $B(\ell^2)$?

Although Kadison and Singer originally thought a negative answer to this question as more probable, in view of its eventual positive answer we will state the conjecture in the affirmative form.

Kadison-Singer Conjecture (KS). *Any pure state on \mathcal{D} extends uniquely to a state on $B(\ell^2)$.*

The first thing to note is that any state $\phi \in \mathfrak{S}(\mathcal{D})$ has a “canonical” extension to $\mathfrak{S}(B(\ell^2))$, given by

$$(2.2) \quad \tilde{\phi}(T) = \phi(\text{diag}(T)).$$

So the problem becomes whether $\tilde{\phi}$ is or not the unique extension of ϕ to $B(\ell^2)$. If ψ is another extension of ϕ and $T \in B(\ell^2)$, then

$$\psi(T - \text{diag } T) = \psi(T) - \phi(\text{diag } T) = \psi(T) - \tilde{\phi}(T).$$

So $\psi = \tilde{\phi}$ if and only if $\psi(T - \text{diag } T) = 0$ for any $T \in B(\ell^2)$, which is equivalent to say that $\psi(T) = 0$ for any $T \in B(\ell^2)$ with $\text{diag } T = 0$. As a consequence, we have the following simple lemma:

Lemma 2.4. *(KS) is true if and only if any extension $\psi \in \mathfrak{S}(B(\ell^2))$ of a pure state on \mathcal{A} satisfies*

$$\text{diag } T = 0 \implies \psi(T) = 0.$$

In fact, pure states of \mathcal{D} can be described more precisely. Indeed, being a commutative algebra, \mathcal{D} is isomorphic to $C(X)$ (as noted in Example 2.1). One can identify X precisely: it is $\beta\mathbb{N}$, the Stone-Čech compactification of \mathbb{N} . We do not need this fact, but will use only a simple observation.

Lemma 2.5. *If ϕ is a pure state on \mathcal{D} and $P \in \mathcal{D}$ is a projection, then $\phi(P)$ is either 0 or 1.*

Proof. It has been noted above (see Example 2.1) that ϕ is multiplicative. Then $\phi(P) = \phi(P^2) = \phi(P)^2$, whence $\phi(P)$ is either 0 or 1. \square

Remark 2.6. As hinted in the introduction, although in the original paper [7] there is no mention of quantum mechanics, in subsequent papers the authors state as source for the problem the work of Dirac on the foundation of quantum mechanics [5]. For some comments on this, see Subsection 9.1 below.

2.3. The Paving Conjecture. Instead of dealing directly with the Kadison–Singer conjecture, we intend to prove a statement about finite dimensional matrices, which is usually known as Anderson’s *paving conjecture* [1]. We use the notation \mathcal{D}_m to indicate diagonal $m \times m$ matrices and diag_m the corresponding map from $M_m(\mathbb{C})$ to \mathcal{D}_m .

Paving Conjecture (PC). *For any $\epsilon > 0$ there exists $r \in \mathbb{N}$ such that the following is true:*

For any $m \in \mathbb{N}$ and $T \in B(\mathbb{C}^m)$ with $\text{diag}_m T = 0$, there exist projections $Q_1, \dots, Q_r \in \mathcal{D}_m$, with $\sum_{i=1}^r Q_i = I_m$, and

$$\|Q_i T Q_i\| \leq \epsilon \|T\|$$

for all $i = 1, \dots, r$.

A diagonal projection $Q \in \mathcal{D}_m$ has its entries 1 or 0, so it is defined by a subset $S \subset \{1, \dots, m\}$. Thus diagonal projections $Q_1, \dots, Q_r \in \mathcal{D}_m$ with $\sum_{i=1}^r Q_i = I_m$ correspond to partitions $\{1, \dots, m\} = S_1 \cup \dots \cup S_r$, $S_i \cap S_j = \emptyset$ for $i \neq j$.

It is important that in the statement of (PC) the number r does not depend on m . This allows us to deduce from (PC) a similar statement, in which \mathbb{C}^m is replaced with the whole ℓ^2 , is also true. We formulate this as a lemma.

Lemma 2.7. *If (PC) is true, then for any $\epsilon > 0$ there exists $r \in \mathbb{N}$ such that, for any $T \in B(\ell^2)$ with $\text{diag } T = 0$ one can find projections $Q_1, \dots, Q_r \in \mathcal{D}$, with $\sum_{i=1}^r Q_i = I$, and*

$$\|Q_i T Q_i\| \leq \epsilon \|T\|$$

for all $i = 1, \dots, r$.

Proof. Embed \mathbb{C}^m canonically into ℓ^2 on the first m coordinates and denote by E_m the corresponding orthogonal projection. For $T \in B(\ell^2)$ denote $T_m = E_m T E_m$. Applying (PC), one finds diagonal projections $Q_1^{(m)}, \dots, Q_r^{(m)}$, such that $\sum_{i=1}^r Q_i^{(m)} = I_m$ and $\|Q_i^{(m)} T_m Q_i^{(m)}\| \leq \epsilon \|T_m\|$.

Now, diagonal projections in $B(\ell^2)$ can be identified with subsets of \mathbb{N} , and therefore with elements in the compact space $\{0, 1\}^{\mathbb{N}}$. In this compact space any sequence has a convergent subsequence; therefore a diagonal argument will produce an increasing subsequence of positive integers m_k , such that for each $i = 1, \dots, r$ we have $Q_i^{(m_k)} \rightarrow Q_i$ for some Q_i . We have

$$\sum_{i=1}^r Q_i = \lim_{k \rightarrow \infty} \sum_{i=1}^r Q_i^{(m_k)} = \lim_{k \rightarrow \infty} I_{m_k} = I.$$

If $\xi, \eta \in \ell^2$ are vectors with finite support, then $\xi, \eta \in \mathbb{C}^{d_k}$ for some k , and then

$$\begin{aligned} |\langle Q_i T Q_i \xi, \eta \rangle| &= |\langle T Q_i \xi, Q_i \eta \rangle| = |\langle T_{m_k} Q_i^{(m_k)} \xi, Q_i^{(m_k)} \eta \rangle| = |\langle Q_i^{(m_k)} T_{m_k} Q_i^{(m_k)} \xi, \eta \rangle| \\ &\leq \|Q_i^{(m_k)} T_{m_k} Q_i^{(m_k)}\| \|\xi\| \|\eta\| \leq \epsilon \|T\| \|\xi\| \|\eta\|. \end{aligned} \quad \square$$

The Paving Conjecture is actually equivalent to the Kadison–Singer Conjecture, but we will need (and prove) only one of the implications.

Proposition 2.8. *The Paving Conjecture implies the Kadison–Singer Conjecture.*

Proof. Fix $\epsilon > 0$, and suppose that r satisfies the conclusion of Lemma 2.7. Take a pure state $\psi \in \mathfrak{S}(B(\ell^2))$ and an operator $T \in B(\ell^2)$ with $\text{diag } T = 0$. By Lemma 2.4 we have to show that $\psi(T) = 0$.

Let Q_i be the diagonal projections associated to T by Lemma 2.7. By Lemma 2.5, $\psi(Q_i) = \phi(Q_i)$ is 0 or 1 for each i . Since $1 = \phi(I) = \sum_{i=1}^r \phi(Q_i)$, it follows that there exists some i_0 for which $\phi(Q_{i_0}) = 1$, while $\phi(Q_i) = 0$ for $i \neq i_0$.

If $i \neq i_0$, then (2.1) implies

$$|\psi(Q_i R)| \leq \psi(Q_i^* Q_i) \psi(R^* R) = \psi(Q_i) \psi(R^* R) = 0,$$

and similarly $\psi(R Q_i) = 0$ for all $R \in B(\ell^2)$. Therefore

$$\psi(T) = \sum_{i=1}^r \sum_{j=1}^r \psi(Q_i T Q_j) = \psi(Q_{i_0} T Q_{i_0}).$$

But the projections Q_i have been chosen such as to have $\|Q_{i_0} T Q_{i_0}\| \leq \epsilon \|T\|$, so

$$|\psi(T)| \leq \|Q_{i_0} T Q_{i_0}\| \leq \epsilon \|T\|.$$

Since this is true for any $\epsilon > 0$, it follows that $\psi(T) = 0$, and the proposition is proved. \square

3. INTERMEZZO: WHAT WE WILL DO NEXT AND WHY

3.1. General plan. As noted above, we intend to prove the Paving Conjecture. The proof will lead us on an unexpected path, so we explain here its main steps.

The Paving Conjecture asks us to find, for a given matrix T , diagonal projections Q_i that achieve certain norm estimates (namely, $\|Q_i T Q_i\| \leq \epsilon \|T\|$). Among the different ways to estimate the norm, the proof in [10] choses a rather unusual one: it uses the fact that the norm of a positive operator is its largest eigenvalue. So we have to consider characteristic polynomials of matrices—in fact, the largest part of the proof is dedicated to estimating roots of such polynomials. (Although it has nothing to do with (KS), one should note the added benefit that we find a way to control with no extra effort all eigenvalues of the matrix, not only the largest one.)

On the other hand, to achieve this control we need to make an unexpected detour: though the characteristic polynomial depends on a single variable, in order to control it one has to go through multivariable polynomials and to use the theory of real stable polynomials as developed by Borcea and Brändén [2]. This may seem unnatural, but it should be mentioned that Borcea and Brändén have already obtained through their methods spectacular results, in particular solving long-standing conjectures in matrix theory that also seemed at first sight to involve just a single complex variable [2, 3]. So maybe one should not be so surprised after all.

A second feature of the proof is its use, at some point, of a random space. After obtaining certain results about eigenvalues of usual matrices, suddenly random matrices appear on the scene. In fact, the use of randomness is not really essential; it rather provides a convenient notation for computing averages. As noted in the previous section, to prove (PC) we need to find a partition of a finite set $\{1, \dots, m\}$ into r subsets with certain properties. The random space eventually considered is finite; its elements are all different such partitions, and no subtle probability is used: all decompositions are assumed to be equally probable. What we will achieve eventually is an estimate on the average of the largest eigenvalue, which will lead to an individual estimate for at least one point of the random space—that is, for one partition. This will be the desired partition.

3.2. Sketch of the proof. We summarize here the development of the proof. As announced above, we intend to discuss the eigenvalues of positive matrices, which are roots of the characteristic polynomial. So we need some preparation concerning polynomials and their roots; this is done first in one variable in Section 4. The main result here is Theorem 4.9, that shows that certain families of polynomials have roots that behave unexpectedly well with respect to averages. This will be used in Section 7 to link eigenvalues of random matrices to their averages.

But we have to go to polynomials in several variables, namely real stable polynomials, which are defined by a condition on their roots. Section 5 is dedicated to real stable polynomials; after presenting their main properties, we are especially interested in some delicate estimate on the location of the roots, which is done through an associated function called the barrier function. The properties of the barrier function represent the most technical and not very transparent part of the proof. The main thing to be used in the sequel is Theorem 5.8, that puts some restriction on the roots of a real stable polynomial.

We apply these facts to characteristic polynomials in Section 6. The voyage through several variables done for polynomials has a correspondent here in the introduction of the *mixed characteristic polynomial*, which depends on several matrices. It happens to be the restriction to one variable of a real stable polynomial, and so Theorem 5.8 can be used in Theorem 6.4 to bound the roots of a mixed characteristic polynomial. Further, this bound translates in a bound for a usual characteristic polynomial in the particular case when the matrices have rank one, since then the mixed characteristic polynomial is precisely the characteristic polynomial of their sum.

Section 7 introduces random matrices; as discussed above, the probability space in view is that of all possible partitions. The main result, Theorem 7.2, uses the results of Section 4 to show that for a sum of independent random matrices of rank one, the eigenvalues of its average yield estimates for the averages of its eigenvalues, and thus for the eigenvalues of at least one point of the probability space. In particular, applying this fact in conjunction with the bound on eigenvalues obtained in Section 6, we will obtain a partition with certain norm properties in Theorem 7.5.

Finally, this last fact is put to good use in Section 8 to obtain a proof of the Paving Conjecture. The first step, that uses Theorem 7.5, obtains for orthogonal projections a quantitative version of (PC). To go from projections to general operators is well known since several decades and may be done in different ways. Here we use a dilation argument taken from [15] to obtain the Paving Conjecture for selfadjoint matrices; going to general matrices is then immediate.

4. ANALYTIC FUNCTIONS AND UNIVARIATE POLYNOMIALS

4.1. Preliminaries. The next theorem in complex function theory is a consequence of Cauchy's argument principle.

Theorem 4.1. *Suppose (f_n) is a sequence of analytic functions on a domain $D \subset \mathbb{C}$, which converges uniformly on compacts to the function $f \not\equiv 0$. If Γ is a simple contour contained in D such that f has no zeros on Γ , then there is $n_0 \in \mathbb{N}$ such for $n \geq n_0$ the number of zeros of f_n and of f in the interior of Γ coincide.*

The next corollary is usually called Hurwitz's Theorem if $m = 1$. The general case follows simply by induction (exercise!).

Corollary 4.2. *Suppose $p_n(z_1, \dots, z_m)$ are polynomials in m variables, such that $p_n \rightarrow p$ uniformly on compacts in some domain $D \subset \mathbb{C}^m$. If p_m has no zeros in D for all m , then either p is identically zero, or it has no zeros in D .*

If f is a polynomial of degree n with all coefficients and all roots real, we denote its roots by

$$\rho_n(f) \leq \dots \leq \rho_1(f).$$

Corollary 4.3. *Suppose $p_s(z) = \sum_{i=1}^n a_i(s)z^i$, with $a_i : I \rightarrow \mathbb{R}$ continuous functions on an interval $I \subset \mathbb{R}$, $a_n(s) \neq 0$ on I . If p_s has real roots for all $s \in I$, then the roots $\rho_1(p_s), \dots, \rho_n(p_s)$ are continuous functions of $s \in I$.*

Proof. We use induction with respect to n . The case $n = 1$ is obvious. Then, for a general n , we prove first that $\rho_1(p_s)$ is continuous, say in $s_0 \in I$. Take $\epsilon > 0$, and suppose also that $p_{s_0}(s_0 \pm \epsilon) \neq 0$. By

continuity of a_i , $p_s(s_0 \pm \epsilon) \neq 0$ for s sufficiently close to s_0 , and so $p_s(z) \neq 0$ for z on the circle Γ of diameter $[s_0 - \epsilon, s_0 + \epsilon]$ (since all p_s have real roots). By Theorem 4.1 all p_s have at least one root inside Γ for s sufficiently close to s_0 . A similar argument, using a circle at the right of $s_0 + \epsilon$, shows that the p_s have no roots larger than b . It follows that $\rho_1(p_s) \in (a, b)$ for s close to s_0 .

If we write now $p_s(z) = (z - \rho_1(p_s))q_s(z)$, then q_s has degree $n - 1$ and continuous coefficients, so its roots are continuous by the induction hypothesis. But we have $\rho_i(p) = \rho_{i-1}(q)$ for $i \geq 2$. \square

Remark 4.4. Even without the assumption that the roots are real, one can prove that there exist continuous functions $\rho_i(s) : I \rightarrow \mathbb{C}$, $i = 1, \dots, n$, such that the roots of p_s are $\rho_1(s), \dots, \rho_n(s)$ for all $s \in I$. The proof is more involved; see, for instance, [8, II.5.2].

We prove next two lemmas about polynomials with real coefficients and real roots.

Lemma 4.5. *Suppose the polynomial p of degree n has real coefficients, real roots, and the leading term positive. Moreover, assume that there exist real numbers $a_{n+1} < a_n < \dots < a_1$ such that $\rho_j(p) \in [a_{j+1}, a_j]$ for all $j = 1, \dots, n$. Then $(-1)^{j-1}p(a_j) \geq 0$ for all $j = 1, \dots, n$.*

In other words, p changes signs (not necessarily strictly) on each of the intervals $[a_{j+1}, a_j]$.

Proof. We will use induction with respect to n . For $n = 1$ the claim is obviously true. Suppose it is true up to $n - 1$, and let p be a polynomial of degree n as in the statement of the lemma. There are two cases to consider.

Suppose first that the roots of p are exactly all points a_j except some a_{j_0} . Then p has only simple roots, so it changes signs in each of them. As $p(x) > 0$ for $x > a_1$, we have $p(x) < 0$ on (a_2, a_1) , etc, up to $(-1)^{j_0-1}p(x) > 0$ on (a_{j_0+1}, a_{j_0-1}) . Therefore $(-1)^{j_0-1}p(a_{j_0}) > 0$; the other inequalities are trivial.

In the remaining case, there is at least one root α of p that is not among the points a_j ; suppose $\alpha \in (a_{j_0}, a_{j_0-1})$. If $p(z) = (z - \alpha)q(z)$, then q has degree $n - 1$ and satisfies the hypotheses of the lemma with respect to the points a_j with $j \neq j_0$. Then $p(a_j)$ has the same sign as $q(a_j)$ for $j < j_0$ and opposite sign for $j > j_0$; from here it follows easily that the correct signs for q (which we know true by the induction hypothesis) produce the correct signs for p . \square

Lemma 4.6. *Suppose the polynomial p has real coefficients and all roots real. Then*

$$(-1)^k \left(\frac{d}{dx} \right)^k \frac{p'}{p}(x) > 0$$

for all $k \in \mathbb{N}$ and $x > \rho_1(p)$.

In particular, $\frac{p'}{p}$ is positive, nonincreasing, and convex for $x > \rho_1(p)$.

Proof. If $p(z) = \prod_{i=1}^n (z - \rho_i(p))$, then $\frac{p'}{p}(z) = \sum_{i=1}^n \frac{1}{z - \rho_i(p)}$, and

$$(-1)^k \left(\frac{d}{dx} \right)^k \frac{p'}{p}(x) = k! \sum_{i=1}^n \frac{1}{(x - \rho_i(p))^{k+1}}.$$

All terms in the last sum are positive for $x > \rho_1(p)$, so the lemma is proved. \square

4.2. Nice families. Suppose $\mathcal{F} = \{f_1, \dots, f_m\}$ is a family of polynomials of the same degree n . We denote

$$\rho_j^+(\mathcal{F}) := \max_{1 \leq i \leq m} \rho_j(f_i), \quad \rho_j^-(\mathcal{F}) := \min_{1 \leq i \leq m} \rho_j(f_i)$$

Definition 4.7. For a family of polynomials $\mathcal{F} = \{f_1, \dots, f_m\}$ of the same degree n a *nice family* iff:

- (1) the coefficient of the dominant term of every f_j is positive;
- (2) every f_j has all roots real;
- (3) for all $j = 2, \dots, n$ we have

$$(4.1) \quad \rho_j^+(\mathcal{F}) \leq \rho_{j-1}^-(\mathcal{F}).$$

The usual formulation (including [10]) is that the f_i s have a common interlacing. Since the actual interlacing polynomial never enters our picture, we prefer this simpler phrasing.

Lemma 4.8. (i) $\{f_1, \dots, f_m\}$ is nice iff every pair $\{f_r, f_s\}$, $r \neq s$, is nice.

(ii) Every subfamily of a nice family is nice.

(iii) If $a \in \mathbb{R}$, then $\mathcal{F} = \{f_1, \dots, f_m\}$ is nice if and only if $\mathcal{G} = \{(x-a)f_1, \dots, (x-a)f_m\}$ is nice.

Proof. (i) and (ii) are immediate. For (iii), there are several cases to consider:

- (1) If $a \in [\rho_{j_0}^-(\mathcal{F}), \rho_{j_0}^+(\mathcal{F})]$ for some j_0 , then

$$\begin{aligned} \rho_j^\pm(\mathcal{G}) &= \rho_j^\pm(\mathcal{F}) \text{ for } j < j_0, \\ \rho_{j_0}^+(\mathcal{G}) &= \rho_{j_0}^+(\mathcal{F}), \quad \rho_{j_0}^-(\mathcal{G}) = \rho_{j_0+1}^+(\mathcal{G}) = 1, \quad \rho_{j_0+1}^-(\mathcal{G}) = \rho_{j_0}^-(\mathcal{F}), \\ \rho_j^\pm(\mathcal{G}) &= \rho_{j-1}^\pm(\mathcal{F}) \text{ for } j > j_0 + 1. \end{aligned}$$

- (2) If $a \in (\rho_{j_0}^+(\mathcal{F}), \rho_{j_0-1}^-(\mathcal{F}))$ for some j_0 , then

$$\begin{aligned} \rho_j^\pm(\mathcal{G}) &= \rho_j^\pm(\mathcal{F}) \text{ for } j < j_0, \\ \rho_{j_0}^\pm(\mathcal{G}) &= a, \\ \rho_j^\pm(\mathcal{G}) &= \rho_{j-1}^\pm(\mathcal{F}) \text{ for } j > j_0. \end{aligned}$$

The formulas in (1) are also valid if $a > \rho_1^+(\mathcal{F})$ (taking $j_0 = 1$) or $a < \rho_n^-(\mathcal{F})$ (taking $j_0 = n + 1$). In all these cases one can easily check that (iii) is true. \square

As a consequence of Lemma 4.8, in order to check that a family is nice we can always assume that it has no common zeros.

The main theorem of this section is the characterization of nice families that follows.

Theorem 4.9. Suppose f_1, \dots, f_m are all polynomials of degree n , with positive dominant coefficients. The following are equivalent:

- (1) $\mathcal{F} = \{f_1, \dots, f_m\}$ is a nice family.
- (2) Any convex combination of f_1, \dots, f_m has only real roots.

If these conditions are satisfied, then for any $j = 1, \dots, n$ we have

$$(4.2) \quad \min_i \rho_j(f_i) \leq \rho_j(f) \leq \max_i \rho_j(f_i)$$

for any convex combination $f = \sum_k t_k f_k$.

Proof. (1) \implies (2). We may suppose by (ii) and (iii) of Lemma 4.8 that all coefficients t_k are positive and that the family has no common zeros. In particular, if we denote $\rho_j^\pm = \rho_j^\pm(\mathcal{F})$, this implies $\rho_j^- < \rho_j^+ \leq \rho_{j-1}^-$ for all j .

We will apply Lemma 4.5 to each of the polynomials f_i and the points $\rho_n^- < \rho_{n-1}^- < \dots < \rho_1^- < \rho_1^+$. We obtain then, for each $i = 1, \dots, m$, that $(-1)^j f_i(\rho_j^-) \geq 0$ for all j , and $f_i(\rho_1^+) \geq 0$.

Fix j ; since the family \mathcal{F} has no common zero, at least one of f_i is nonzero in ρ_j^- , and so $(-1)^j f(\rho_j^-) > 0$. Similarly, $f(\rho_1^+) > 0$. Therefore on each of the intervals (ρ_j^-, ρ_{j-1}^-) , as well as on (ρ_1^-, ρ_1^+) , f changes sign (strictly), and therefore must have a root in the interior. Since there are n intervals, we have thus found n roots of f , and so all its roots are real. Moreover, we have obtained $\rho_j(f) > \rho_j^-$ for all j .

On the other hand, we might have used, in applying Lemma 4.5 to the polynomials f_i , the points $\rho_n^- < \rho_n^+ < \rho_{n-1}^+ < \dots < \rho_1^+$ instead of $\rho_n^- < \rho_{n-1}^- < \dots < \rho_1^- < \rho_1^+$. A similar argument yields then $\rho_j(f) < \rho_j^+$ for all j . Therefore the inequalities (4.2) are proved.

(2) \implies (1). According to Lemma 4.8 it is enough to prove the implication for two functions f_1, f_2 , and we may also suppose that they have no common roots. Fix $2 \leq j \leq n$; we have to prove that $\rho_j^+ \leq \rho_{j-1}^-$. Denote $f_t = t f_1 + (1-t) f_2$ ($0 \leq t \leq 1$). By Corollary 4.3 the function $t \mapsto \rho_j(f_t)$ is continuous on $[0, 1]$ and takes only real values; so its values for $0 < t < 1$ cover the interval (ρ_j^-, ρ_j^+) . It follows that this interval cannot contain a root of either f_1 or f_2 , since a common root of, say, f_1 and f_t is also a root of f_2 .

Suppose then first that f_1 and f_2 have only simple roots. Then the intervals $[\rho_j^-, \rho_j^+]$ and $[\rho_{j-1}^-, \rho_{j-1}^+]$ have all four endpoints disjoint, and by definition $\rho_j^- < \rho_{j-1}^-$. If $\rho_{j-1}^- \in (\rho_j^-, \rho_j^+)$, this would contradict the conclusion of the preceding paragraph. So $\rho_{j-1}^- > \rho_j^+$ and (4.1) is proved.

To obtain the general case, note first that f_t has all roots simple for $0 < t < 1$. Indeed, a multiple solution x of $f_t = 0$ would also be a multiple solution of $\frac{f_2}{f_1} = \frac{t}{t-1}$. But it is easy to see (draw the graph!) that then $\frac{f_2}{f_1} = \frac{t'}{t'-1}$ has a single root in some interval $(x - \epsilon, x + \epsilon)$ for at least some t' close to t (slightly larger or slightly smaller). However, from Theorem 4.1 it follows that $f_{t'}$ has more than one root in the disc $|z - x| < \epsilon$, and so $f_{t'}$ would not have all roots real.

To end the proof, we apply the first step to f_ϵ and $f_{1-\epsilon}$ ($\epsilon > 0$), which have only simple roots. Then we let $\epsilon \rightarrow 0$ and use Corollary 4.3 to obtain inequality (4.1). \square

5. SEVERAL VARIABLES: REAL STABLE POLYNOMIALS

5.1. General facts. Denote $\mathbb{H} = \{z \in \mathbb{C} : \Im z > 0\}$.

Definition 5.1. A polynomial $p(z_1, \dots, z_m)$ is called *real stable* if it has real coefficients and it has no zeros in \mathbb{H}^m .

In case $m = 1$ a real stable polynomial is a polynomial that has real coefficients and real zeros. Genuine examples in several variables are produced by the next lemma.

Lemma 5.2. *If $A_1, \dots, A_m \in M_d(\mathbb{C})$ are positive matrices, then the polynomial*

$$(5.1) \quad q(z, z_1, \dots, z_m) = \det(zI_d + \sum_{i=1}^m z_i A_i)$$

is real stable.

Proof. It is immediate from the definition that

$$q(\bar{z}, \bar{z}_1, \dots, \bar{z}_m) = \overline{q(z, z_1, \dots, z_m)},$$

whence the coefficients of q are real.

Assume that $q(z, z_1, \dots, z_m) = 0$, and $\Im z, \Im z_i > 0$. Since $zI_d + \sum_{i=1}^m z_i A_i$ is not invertible, there exists $\xi \in \mathbb{C}^d, \xi \neq 0$, such that

$$0 = \langle (zI_d + \sum_{i=1}^m z_i A_i) \xi, \xi \rangle = z \|\xi\|^2 + \sum_{i=1}^m z_i \langle A_i \xi, \xi \rangle,$$

and so

$$0 = \Im z \|\xi\|^2 + \sum_{i=1}^m \Im z_i \langle A_i \xi, \xi \rangle.$$

This is a contradiction, since $\Im z \|\xi\|^2 > 0$ and $\Im z_i \langle A_i \xi, \xi \rangle \geq 0$ for all i . \square

The next theorem gives the basic properties of real stable polynomials. Denote, for simplicity, by ∂_i the partial derivative $\frac{\partial}{\partial z_i}$.

Theorem 5.3. *Suppose p is a real stable polynomial.*

- (i) *If $m > 1$ and $t \in \mathbb{R}$, then $p(z_1, \dots, z_{m-1}, t)$ is either real stable or identically zero.*
- (ii) *If $t \in \mathbb{R}$, then $(1 + t\partial_m)p$ is real stable.*

Proof. (i) Obviously $p(z_1, \dots, z_{m-1}, t)$ has real coefficients. Suppose it is not identically zero. If $\Im w > 0$ is fixed, then the polynomial $p(z_1, \dots, z_{m-1}, w)$ is real stable by definition. Therefore all polynomials $p(z_1, \dots, z_{m-1}, t + \frac{i}{n})$ (for $n \in \mathbb{N}$) are real stable. We let then $n \rightarrow \infty$ and apply Corollary 4.2 to $D = \mathbb{H}^m$ to obtain the desired result.

(ii) We may assume $t \neq 0$ (otherwise there is nothing to prove). Suppose $(1 + t\partial_m)p(z_1, \dots, z_m) = 0$ for some $(z_1, \dots, z_m) \in \mathbb{H}^m$. Since p is real stable, $p(z_1, \dots, z_m) \neq 0$. The one-variable polynomial $q(z) := p(z_1, \dots, z_{m-1}, z)$ has no roots with positive imaginary part (in particular, $q(z_m) \neq 0$), so we may write

$$q(z) = c \prod_{i=1}^n (z - w_i), \quad \Im w_i \leq 0.$$

Therefore

$$0 = (1 + t\partial_m)p(z_1, \dots, z_m) = (q + tq')(z_m) = q(z_m) \left(1 + t \frac{q'(z_m)}{q(z_m)} \right),$$

and, since $q(z_m) \neq 0$,

$$0 = 1 + t \sum_{i=1}^n \frac{1}{z_m - w_i} = 1 + t \sum_{i=1}^n \frac{\overline{z_m - w_i}}{|z_m - w_i|^2}.$$

Taking the imaginary part, we obtain

$$t \sum_{i=1}^n \frac{\Im w_i - \Im z_m}{|z_m - w_i|^2} = 0$$

which is a contradiction, since $t \neq 0$ and $\Im w_i - \Im z_m < 0$ for all i . \square

We will also need a lemma that uses a standard result in algebraic geometry, namely Bézout's Theorem (which can be found in any standard text).

Lemma 5.4. *Suppose $p(z, w)$ is a nonconstant polynomial in two variables, of degree n in w , which is irreducible over \mathbb{R} . There is a finite set $F \in \mathbb{C}$ such that, if $p(z_0, w_0) = 0$ and $z_0 \notin F$, then:*

- (1) *the equation $p(z_0, w) = 0$ has n distinct solutions;*
- (2) *for each of these solutions (z_0, w_0) we have $\frac{\partial p}{\partial w}(z_0, w) \neq 0$.*

Proof. First, if $p(z, w) = q(z)w^n + \dots$, then the roots of q form a finite set F_1 .

Secondly, if p is irreducible, then p and $\frac{\partial p}{\partial w}$ are coprime over \mathbb{R} , and hence also over \mathbb{C} . Bézout's Theorem in algebraic geometry states that two curves defined by coprime equations have only a finite number of common points, so this is true about the sets defined by $p(z, w) = 0$ and $\frac{\partial p}{\partial w}(z, w) = 0$. Let F_2 be the set of the projections of these points onto the first coordinate. The set $F = F_1 \cup F_2$ has the required properties. \square

5.2. The barrier function. Our eventual purpose in this subsection is to obtain estimates on the roots of real stable polynomials; more precisely, we want to show that a restriction on the roots of a real stable polynomial p may imply a restriction on the roots of $(1 - \partial_i)p$ (which is also real stable by Theorem 5.3).

We will often use the restriction of a polynomial in m complex variables to $\mathbb{R}^m \subset \mathbb{C}^m$. To make things easier to follow, we will be consistent in this subsection with the following notation: z, w will belong to \mathbb{C}^m (and corresponding subscripted letters in \mathbb{C}), while x, y, s, t will be in \mathbb{R}^m (and corresponding subscripted letters in \mathbb{R}). If $x = (x_1, \dots, x_m) \in \mathbb{R}^m$, then $\{y \geq x\}$ will denote $\{y = (y_1, \dots, y_m) \in \mathbb{R}^m : y_i \geq x_i \text{ for all } i = 1, \dots, m\}$.

The main tool is a certain function associated to p called the *barrier function*, whose one-dimensional version has already been met in Lemma 4.6. It is defined wherever $p \neq 0$ by $\Phi_p^i = \frac{\partial_i p}{p}$; if $p(x) > 0$ it can also be written as $\Phi_p^i(x) = \partial_i(\log p)(x)$. The argument of the barrier function will always actually be in \mathbb{R}^m .

The connection of the barrier function with our problem is given by the simple observation that if $p(x) \neq 0$ and $(1 - \partial_i)p(x) = 0$, then $\Phi_p^i(x) = 1$. So, in particular, a set on which $0 \leq \Phi_p^i < 1$ does not contain zeros of $(1 - \partial_i)p$. To determine such sets, the basic result is the next lemma, which is a multidimensional extension of Lemma 4.6.

Lemma 5.5. *Suppose $x \in \mathbb{R}^m$, and $p(z_1, \dots, z_m)$ is a real stable polynomial that has no roots in $\{y \geq x\}$, then*

$$(-1)^k \frac{\partial^k}{\partial z_j^k} \Phi_p^i(x') \geq 0$$

for any $k \geq 0$, $1 \leq i, j \leq m$, and $x' \geq x$.

In particular, if e_j is one of the canonical basis vectors in \mathbb{C}^m , then $t \mapsto \Phi_p^i(x + te_j)$ is positive, nonincreasing and convex on $[0, \infty]$.

Proof. The assertion reduces to Lemma 4.6 for $m = 1$ or for $k = 0$; and also for $i = j$, since then fixing all variables except the i th reduces the problem to the one variable case.

In the general case, it is enough to do it for $y = x$, since if p has no roots in $\{y \geq x\}$, then it has no roots in $\{y \geq x'\}$ for all $x' \geq x$. By fixing all variables except i and j , we may assume that $m = 2$, $i = 1, j = 2, k \geq 1$. Moreover, we may also assume that $p > 0$ on $\{y \geq x\}$ (otherwise we work with $-p$, since $\Phi_p^i = \Phi_{-p}^i$).

So we have to prove that, if $p(z_1, z_2)$ is a real stable polynomial which has no zeros in $\{y_1 \geq x_1, y_2 \geq x_2\}$, then

$$0 \leq (-1)^k \frac{\partial^k}{\partial z_2^k} \Phi_p^1(x_1, x_2) = (-1)^k \frac{\partial^k}{\partial z_2^k} \left(\frac{\partial}{\partial z_1} \log p \right) (x_1, x_2) = \frac{\partial}{\partial z_1} \left((-1)^k \frac{\partial^k}{\partial z_2^k} \log p \right) (x_1, x_2).$$

We will in fact prove that the map

$$t \mapsto (-1)^k \frac{\partial^k}{\partial z_2^k} \log p(t, x_2)$$

is increasing for $t \geq x_1$. It is enough to achieve this for p irreducible over \mathbb{R} , since, if $p = p_1 p_2$ is real stable and has no roots in $\{y \geq x\}$, then the same is true for p_1 and p_2 , and obviously

$$(-1)^k \frac{\partial^k}{\partial z_2^k} \log p(t, x_2) = (-1)^k \frac{\partial^k}{\partial z_2^k} \log p_1(t, x_2) + (-1)^k \frac{\partial^k}{\partial z_2^k} \log p_2(t, x_2).$$

Suppose then that p is irreducible. For $t \geq x_1$ fixed, the polynomial $p(t, z)$ is real stable, and thus has all roots real; denote them, as in Section 4, by $\rho_1(t) \geq \dots \geq \rho_n(t)$.

Applying to p Lemma 5.4, take $t \geq x_1$ that does not belong to the finite set F therein. The functions $\rho_i(t)$ are therefore differentiable in t , and we have

$$(5.2) \quad p(t, z) = c(t) \prod_{i=1}^n (z - \rho_i(t))$$

Therefore

$$(5.3) \quad \begin{aligned} \left((-1)^k \frac{\partial^k}{\partial z_2^k} \log p \right) \left((-1)^k \frac{\partial^k}{\partial z_2^k} \log p \right) (t, x_2) &= (-1)^k \frac{\partial^k}{\partial z_2^k} \left(\sum_{i=1}^n \log(z - \rho_i(t)) \right) \Big|_{z=x_2} \\ &= - \sum_{i=1}^n \frac{(k-1)!}{(x_2 - \rho_i(t))^k}. \end{aligned}$$

If $t \geq x_1$, we cannot have $\rho_i(t) \geq x_2$ since then $(t, \rho_i(t))$ would be a root of p in $\{y \geq x\}$, contrary to the assumption. Thus $x_2 - \rho_i(t) > 0$, and in order to show that the function in (5.3) is increasing, it is enough to show that $t \mapsto \rho_i(t)$ is decreasing for $t \geq x_1$ and all i .

Now all ρ_i s are differentiable for $t \geq x_1, t \notin F$. To show that they are decreasing, it is enough to show that $\rho_i'(t) \leq 0$ for such t . Suppose then that there exists $i \in \{1, \dots, n\}$ and $t \geq x_1$ such that $\rho_i'(t) > 0$; let $s = \rho_i(t)$. Since $\frac{\partial p}{\partial z_2}(t, s) \neq 0$, we may apply the (complex) implicit function theorem in a neighborhood of (t, s) (in \mathbb{C}^2). We obtain that the solutions of $p(z_1, z_2) = 0$ therein are of the form $(z_1, g(z_1))$ for some locally defined analytic function of one variable g , which by analytic

continuation has to be an extension of ρ to a complex neighborhood of t . So $g'(t) = \rho'_i(t)$, and in the neighborhood of t we have

$$g(z_1) = t + \rho'_i(t)(z_1 - t) + O(|z_1 - t|^2).$$

If $\Im z_1 > 0$ and small, one also has $\Im g(z_1) > 0$. We obtain thus the zero $(z_1, g(z_1))$ of p in \mathbb{H}^2 , contradicting the real stability of p . This ends the proof of the lemma. \square

Corollary 5.6. *Suppose $x \in \mathbb{R}^m$, and p is a real stable polynomial, without zeros in $\{y \geq x\}$. Then $\Phi_p^j(y) \leq \Phi_p^j(x)$ for any $y \geq x$ and $j = 1, \dots, m$.*

Proof. If p has no zeros in $\{y \geq x\}$, obviously it has no zeros in $\{y \geq x'\}$ for any $x' \geq x$. Therefore, by Lemma 5.5, the function $t \mapsto \Phi_p^j(x' + te_i)$ is nonincreasing on $[0, \infty)$ for any $i = 1, \dots, m$. We have then

$$\Phi_p^j(x_1, \dots, x_m) \geq \Phi_p^j(y_1, x_2, \dots, x_m) \geq \Phi_p^j(y_1, y_2, x_3, \dots, x_m) \geq \dots \geq \Phi_p^j(y_1, \dots, y_m) \quad \square$$

The main monotonicity and convexity properties of Φ_p^i are put to work in the next lemma to obtain a restriction on the location of zeros of $(1 - \partial_j)p$. As noted above, we will use the condition $\Phi_p^j < 1$, but in a more precise variant which will lends itself to iteration.

Lemma 5.7. *Let $x \in \mathbb{R}^m$, and p a real stable polynomial, without zeros in $\{y \geq x\}$. Suppose also that*

$$\Phi_p^j(x) + \frac{1}{\delta} \leq 1$$

for some $j \in \{1, \dots, m\}$ and $\delta > 0$.

Then:

- (i) $(1 - \partial_j)p$ has no zeros in $\{y \geq x\}$.
- (ii) For any $i = 1, \dots, m$ we have

$$\Phi_{(1-\partial_j)p}^i(x + \delta e_j) \leq \Phi_p^i(x).$$

Proof. By Corollary 5.6 we have

$$\frac{\partial_j p(y)}{p(y)} = \Phi(y) \leq \Phi(x) \leq 1 - \frac{1}{\delta} < 1,$$

so $\partial_j p(y) \neq p(y)$, or $(1 - \partial_j)p(y) \neq 0$.

To prove (ii), note first that $(1 - \partial_j)p = p(1 - \Phi_p^j)$, whence $\log[(1 - \partial_j)p] = \log p + \log(1 - \Phi_p^j)$, so, by differentiating,

$$\Phi_{(1-\partial_j)p}^i = \Phi_p^i - \frac{\partial_i \Phi_p^j}{1 - \Phi_p^j}.$$

The required inequality becomes then

$$(5.4) \quad -\frac{\partial_i \Phi_p^j(x + \delta e_j)}{1 - \Phi_p^j(x + \delta e_j)} \leq \Phi_p^i(x) - \Phi_p^i(x + \delta e_j).$$

By Corollary 5.6 we have

$$\Phi_p^j(x + \delta e_j) \leq \Phi_p^j(x) \leq 1 - \frac{1}{\delta},$$

or

$$\frac{1}{1 - \Phi_p^j(x + \delta e_j)} \leq \delta.$$

Further on, p has no zeros in $\{y \geq x + \delta e_j\}$, so Lemma 5.5 (applied in $x + \delta e_j$) implies, in particular, that $-\partial_i \Phi_p^j(x + \delta e_j) \geq 0$, whence

$$-\frac{\partial_i \Phi_p^j(x + \delta e_j)}{1 - \Phi_p^j(x + \delta e_j)} \leq -\delta \partial_i \Phi_p^j(x + \delta e_j).$$

To prove (5.4), it is then enough to show that

$$-\delta \partial_i \Phi_p^j(x + \delta e_j) \leq \Phi_p^i(x) - \Phi_p^i(x + \delta e_j).$$

Using $\partial_i \Phi_p^j(x + \delta e_j) = \partial_j \Phi_p^i(x + \delta e_j)$, the inequality can be written

$$\Phi_p^i(x + \delta e_j) \leq \Phi_p^i(x) + \delta \partial_j \Phi_p^i(x + \delta e_j).$$

This, however, is an immediate consequence of the convexity of the function $t \mapsto \Phi_p^i(x + te_j)$, that has been proved in Lemma 5.5. \square

Finally, the next theorem is the main result of this section that we will use in the sequel.

Theorem 5.8. *Let $x \in \mathbb{R}^m$, and p a real stable polynomial, without zeros in $\{y \geq x\}$. Suppose also that*

$$\Phi_p^j(x_1, \dots, x_m) + \frac{1}{\delta} \leq 1$$

for some $\delta > 0$ and $j = 1, \dots, m$. Then

$$\prod_{i=1}^m (1 - \partial_i) p$$

has no zeros in $\{y \geq x + \tilde{\delta}\}$, where $\tilde{\delta} := (\delta, \dots, \delta) \in \mathbb{R}^m$.

Proof. The proof follows by applying Lemma 5.7 successively to $j = 1$ and x , then to $j = 2$ and $x + \delta e_1$, etc. \square

6. CHARACTERISTIC AND MIXED CHARACTERISTIC POLYNOMIALS

6.1. Mixed characteristic polynomial. We intend now to apply the results of Section 5 to polynomials related to matrices. Our final goal is to estimate eigenvalues; that is, roots of the characteristic polynomial. But we will first consider another polynomial, attached to a tuple of matrices.

Definition 6.1. If $A_1, \dots, A_m \in M_d(\mathbb{C})$, then the *mixed characteristic polynomial* of the matrices A_i is defined by the formula

$$(6.1) \quad \mu[A_1, \dots, A_m](z) = \prod_{i=1}^m (1 - \partial_i) \det(zI_d + \sum_{i=1}^m z_i A_i) \Big|_{z_1 = \dots = z_m = 0}.$$

It is easily seen that if we fix $m - 1$ of the matrices A_1, \dots, A_m , then $\mu[A_1, \dots, A_m](z)$ is of degree 1 in the entries of the remaining matrix. Indeed, if we develop the determinant that enters (6.1), then any term that contains a product of, say, k entries of A_j has also the factor z_j^k . If we apply $(1 - \partial_j)$, we are left with z_j^{k-1} , and if $k \geq 2$ this term becomes 0 if $z_j = 0$.

Example 6.2. For one or two matrices we have

$$\begin{aligned}\mu[A_1](z) &= z^d - z^{d-1} \operatorname{Tr} A_1 \quad \text{if } m = 1, \\ \mu[A_1, A_2](z) &= z^d - z^{d-1}(\operatorname{Tr} A_1 + \operatorname{Tr} A_2) + z^{d-2}(\operatorname{Tr} A_1 \operatorname{Tr} A_2 - \operatorname{Tr}(A_1 A_2)) \quad \text{if } m = 2.\end{aligned}$$

In the general case, the coefficients of $\mu[A_1, \dots, A_m](z)$ are certain expressions in the traces of monomials in A_1, \dots, A_m that are well known in the invariant theory of matrices (see [13]).

The results in Section 5 have consequences for the mixed characteristic polynomials.

Theorem 6.3. *Suppose $A_1, \dots, A_m \in M_d(\mathbb{C})$ are positive matrices. Then $\mu[A_1, \dots, A_m](z)$ has only real roots.*

Proof. We have seen in Lemma 5.2 that the polynomial q defined by (5.1) is real stable. But $\mu[A_1, \dots, A_m]$ is obtained from q by first applying $(1 - \partial_i)$ for $i = 1, \dots, m$ and then specializing to $z_1 = \dots = z_m = 0$. By Theorem 5.3, these operations preserve the real stable character. So $\mu[A_1, \dots, A_m]$ is a real stable polynomial of one variable, which means exactly that it has real roots. \square

Remember Jacobi's formula for the derivative of the determinant of an invertible matrix:

$$(6.2) \quad \frac{(\det M(t))'}{\det M(t)} = \operatorname{Tr} \left(M(t)^{-1} M'(t) \right).$$

Theorem 6.4. *Suppose $A_1, \dots, A_m \in M_d(\mathbb{C})$ are positive matrices, such that $\sum_{i=1}^m A_i = I_d$ and $\operatorname{Tr} A_i \leq \epsilon$ for each $i = 1, \dots, m$. Then any root of $\mu[A_1, \dots, A_m]$ is smaller than $(1 + \sqrt{\epsilon})^2$.*

Proof. The polynomial

$$p(z) := \det\left(\sum_{i=1}^m z_i A_i\right).$$

is real stable, being the specialization of the polynomial q in (5.1) to $z = 0$. If $t > 0$ and $\tilde{t} := (t, \dots, t) \in \mathbb{C}^d$, then, for $y \geq \tilde{t}$ we have $\sum_{i=1}^m y_i A_i \geq \sum_{i=1}^m t A_i = t I_d$. Therefore $\sum_{i=1}^m y_i A_i$ is invertible, and $p(y) \neq 0$.

We may apply Jacobi's formula (6.2) in order to compute the barrier function Φ_p^j , and we obtain

$$\Phi_p^j(x_1, \dots, x_m) = \operatorname{Tr}\left(\left(\sum_{i=1}^m x_i A_i\right)^{-1} A_j\right).$$

In particular, if $t > 0$, then

$$\Phi_p^j(t, \dots, t) = \operatorname{Tr}(t^{-1} A_j) \leq \frac{\epsilon}{t}.$$

It follows then from Theorem 5.8 that, if we $t, \delta > 0$ are such that $\frac{\epsilon}{t} + \frac{1}{\delta} \leq 1$, then $\prod_{i=1}^m (1 - \partial_i) p$ has no zeros in $\{y \geq (t + \delta, \dots, t + \delta)\}$. The choice $t = \epsilon + \sqrt{\epsilon}$, $\delta = 1 + \sqrt{\epsilon}$ (which can easily be shown to be optimal) yields $t + \delta = (1 + \sqrt{\epsilon})^2$, and therefore p has no roots y with $y_i \geq (1 + \sqrt{\epsilon})^2$ for all i .

Now, using the relation $\sum_{i=1}^m A_i = 1$, one obtains

$$\begin{aligned} \mu[A_1, \dots, A_m](z) &= \prod_{i=1}^m (1 - \partial_i) \det(zI_d + \sum_{i=1}^m z_i A_i) \Big|_{z_1=\dots=z_m=0} \\ &= \prod_{i=1}^m (1 - \partial_i) \det\left(\sum_{i=1}^m w_i A_i\right) \Big|_{w_1=\dots=w_m=z} \\ &= \prod_{i=1}^m (1 - \partial_i) p(z, z, \dots, z), \end{aligned}$$

which cannot be zero if $z \geq (1 + \sqrt{\epsilon})^2$. Therefore all roots of μ are smaller than $(1 + \sqrt{\epsilon})^2$. \square

6.2. Decomposing in rank one matrices and the characteristic polynomial. In an important particular case the mixed characteristic polynomial coincides with a usual characteristic polynomial. Remember this is defined, for $A \in M_d(\mathbb{C})$, by $p_A(z) = \det(zI_d - A)$.

Lemma 6.5. *Suppose $B, A_1, \dots, A_m \in M_d(\mathbb{C})$, and A_1, \dots, A_m have rank one. Then the polynomial*

$$(z_1, \dots, z_m) \mapsto \det(B + z_1 A_1 + \dots + z_m A_m)$$

is of degree ≤ 1 separately in each variable.

Proof. By fixing all the variables except one, we have to show that, for any $B, A_1 \in M_d(\mathbb{C})$, A_1 of rank one, the function

$$z \mapsto \det(B + z A_1)$$

is of degree at most 1. This is obvious if we choose a basis in which the first vector spans the image of A_1 , and we develop the determinant with respect to the first row. \square

Suppose now $p(z_1, \dots, z_m)$ is a polynomial of degree ≤ 1 separately in each variable. Then p is equal to its Taylor expansion at the origin of order 1 in each variable, that is:

$$p(z_1, \dots, z_m) = \sum_{\epsilon_i \in \{0,1\}} c_{\epsilon_1, \dots, \epsilon_m} z_1^{\epsilon_1} \dots z_m^{\epsilon_m},$$

with

$$c_{\epsilon_1, \dots, \epsilon_m} = \partial_1^{\epsilon_1} \dots \partial_m^{\epsilon_m} p(w_1, \dots, w_m) \Big|_{w_1=\dots=w_m=0}.$$

Therefore

$$\begin{aligned} p(z_1, \dots, z_m) &= \sum_{\epsilon_i \in \{0,1\}} z_1^{\epsilon_1} \dots z_m^{\epsilon_m} \partial_1^{\epsilon_1} \dots \partial_m^{\epsilon_m} p(w_1, \dots, w_m) \Big|_{w_1=\dots=w_m=0} \\ &= \prod_{i=1}^m (1 + z_i \partial_i) p(w_1, \dots, w_m) \Big|_{w_1=\dots=w_m=0}. \end{aligned}$$

In the case of the polynomial in Lemma 6.5, this formula becomes

$$\det(B + \sum_{i=1}^m z_i A_i) = \prod_{i=1}^m (1 + z_i \partial_i) \det(B + \sum_{i=1}^m w_i A_i) \Big|_{w_1=\dots=w_m=0}.$$

In fact, we are interested by this last formula precisely when $B = zI_d$ and all $z_i = -1$. We obtain then the next theorem.

Theorem 6.6. Suppose $A_1, \dots, A_m \in M_d(\mathbb{C})$ have rank one. If $A = A_1 + \dots + A_m$, then

$$p_A(z) = \mu[A_1, \dots, A_m](z).$$

Remark 6.7. The mixed characteristic polynomial and the usual characteristic polynomial are invariant with respect to a change of basis. So, although we have spoken about matrices for convenience, the statements of Theorems 6.4 and 6.6 can be stated for $A_1, \dots, A_m \in \mathcal{L}(V)$, where $\mathcal{L}(V)$ denotes the space of linear operators on the finite dimensional vector space V .

7. RANDOMISATION

7.1. Random matrices and determinants. Let (Ω, \mathbf{p}) be a finite probability space. If X is a random variable on Ω , the *expectation* (or *average*) of $\mathbb{E}(X)$ is defined, as usually, by

$$\mathbb{E}(X) := \sum_{\omega \in \Omega} \mathbf{p}(\omega) X(\omega).$$

If X_1, \dots, X_m are *independent* random variables, then, in particular, we have

$$(7.1) \quad \mathbb{E}(X_1 \cdots X_m) = \mathbb{E}(X_1) \cdots \mathbb{E}(X_m).$$

We will use random matrices $\mathbf{A}(\omega) \in M_d(\mathbb{C})$, whose entries are random variables; then $\mathbb{E}(\mathbf{A})$ is the matrix whose entries are the expectations of the corresponding entries of \mathbf{A} . The random matrices $\mathbf{A}_1, \mathbf{A}_2$ are called independent if any entry of \mathbf{A}_1 is independent of every entry of \mathbf{A}_2 . Also, when we say that a random matrix $\mathbf{A}(\omega)$ has rank one, this means that $\mathbf{A}(\omega)$ has rank one for any $\omega \in \Omega$.

The characteristic polynomial $p_{\mathbf{A}}$ of a random matrix \mathbf{A} is also a random variable, by which we mean that its coefficients are random variables. Then the polynomial $\mathbb{E}(p_{\mathbf{A}})$ has as coefficients the expectations of the coefficients of \mathbf{A} .

Theorem 7.1. Suppose $\mathbf{A}_1(\omega), \dots, \mathbf{A}_m(\omega)$ are independent rank one random matrices in $M_d(\mathbb{C})$, and $\mathbf{A} = \mathbf{A}_1 + \dots + \mathbf{A}_m$. Then

$$\mathbb{E}(p_{\mathbf{A}}) = \mu[\mathbb{E}(\mathbf{A}_1), \dots, \mathbb{E}(\mathbf{A}_m)].$$

Proof. By Theorem 6.6 we have, for each $\omega \in \Omega$, $p_{\mathbf{A}(\omega)} = \mu[\mathbf{A}_1(\omega), \dots, \mathbf{A}_m(\omega)]$. By taking expectations,

$$\mathbb{E}(p_{\mathbf{A}}) = \mathbb{E}(\mu[\mathbf{A}_1(\omega), \dots, \mathbf{A}_m(\omega)]).$$

Now independence of \mathbf{A}_i s combined with the multilinearity of μ implies that

$$\mathbb{E}(\mu[\mathbf{A}_1(\omega), \dots, \mathbf{A}_m(\omega)]) = \mu[\mathbb{E}(\mathbf{A}_1), \dots, \mathbb{E}(\mathbf{A}_m)],$$

which ends the proof. □

We can say more if we also assume that the \mathbf{A}_i s are all positive.

Theorem 7.2. Suppose $\mathbf{A}_1(\omega), \dots, \mathbf{A}_m(\omega)$ are independent rank one positive random matrices in $M_d(\mathbb{C})$, and $\mathbf{A} = \mathbf{A}_1 + \dots + \mathbf{A}_m$. Then, for any $j = 1, \dots, d$, we have

$$\min_{\omega \in \Omega} \rho_j(p_{\mathbf{A}(\omega)}) \leq \rho_j(\mu[\mathbb{E}(\mathbf{A}_1), \dots, \mathbb{E}(\mathbf{A}_m)]) \leq \max_{\omega \in \Omega} \rho_j(p_{\mathbf{A}(\omega)}).$$

Proof. We prove only the left hand side inequality; the right hand side is similar. It is enough to show that for any $i = 1, \dots$ we have

$$(7.2) \quad \begin{aligned} \min_{\omega \in \Omega} \rho_j(\mu[\mathbf{A}_1(\omega), \dots, \mathbf{A}_{i-1}(\omega), \mathbf{A}_i(\omega), \mathbb{E}(\mathbf{A}_{i+1}), \dots, \mathbb{E}(\mathbf{A}_m)]) \\ \leq \min_{\omega \in \Omega} \rho_j(\mu[\mathbf{A}_1(\omega), \dots, \mathbf{A}_{i-1}(\omega), \mathbb{E}(\mathbf{A}_i), \mathbb{E}(\mathbf{A}_{i+1}), \dots, \mathbb{E}(\mathbf{A}_m)]). \end{aligned}$$

Indeed, for $i = m$ the left hand side coincides with $\min_{\omega \in \Omega} \rho_j(p_{\mathbf{A}(\omega)})$ by Theorem 6.6, while for $i = 1$ the right hand side is precisely $\rho_j(\mu[\mathbb{E}(\mathbf{A}_1), \dots, \mathbb{E}(\mathbf{A}_m)])$. The chain of inequalities corresponding to $i = 1, 2, \dots, m$ proves then the theorem.

Fix then i and $\omega \in \Omega$, and consider the family of polynomials

$$f_{\omega'} = \mu[\mathbf{A}_1(\omega), \dots, \mathbf{A}_{i-1}(\omega), \mathbf{A}_i(\omega'), \mathbb{E}(\mathbf{A}_{i+1}), \dots, \mathbb{E}(\mathbf{A}_m)], \quad \omega' \in \Omega.$$

Take $c_{\omega'} \geq 0$, with $\sum_{\omega' \in \Omega} c_{\omega'} = 1$. By the multilinearity of the mixed characteristic polynomial, we have

$$\begin{aligned} \sum_{\omega' \in \Omega} c_{\omega'} f_{\omega'} &= \sum_{\omega' \in \Omega} c_{\omega'} \mu[\mathbf{A}_1(\omega), \dots, \mathbf{A}_{i-1}(\omega), \mathbf{A}_i(\omega'), \mathbb{E}(\mathbf{A}_{i+1}), \dots, \mathbb{E}(\mathbf{A}_m)] \\ &= \mu[\mathbf{A}_1(\omega), \dots, \mathbf{A}_{i-1}(\omega), \sum_{\omega' \in \Omega} c_{\omega'} \mathbf{A}_i(\omega'), \mathbb{E}(\mathbf{A}_{i+1}), \dots, \mathbb{E}(\mathbf{A}_m)]. \end{aligned}$$

Since the last polynomial is the mixed characteristic polynomial of positive matrices, it has all roots real by Theorem 6.3. It follows by Theorem 4.9 that $\{f_{\omega'} : \omega' \in \Omega\}$ is a nice family. Moreover, if we take as coefficients of the convex combination $c_{\omega'} = \mathbf{p}(\omega')$ and so for any $j = 1, \dots, d$ we have $\sum_{\omega' \in \Omega} c_{\omega'} \mathbf{A}_i(\omega') = \mathbb{E}(\mathbf{A}_i)$. Applying the last part of Theorem 4.9 it follows that for any $j = 1, \dots, d$,

$$\begin{aligned} \min_{\omega' \in \Omega} \rho_j(\mu[\mathbf{A}_1(\omega), \dots, \mathbf{A}_{i-1}(\omega), \mathbf{A}_i(\omega'), \mathbb{E}(\mathbf{A}_{i+1}), \dots, \mathbb{E}(\mathbf{A}_m)]) \\ \rho_j(\mu[\mathbf{A}_1(\omega), \dots, \mathbf{A}_{i-1}(\omega), \mathbb{E}(\mathbf{A}_i), \mathbb{E}(\mathbf{A}_{i+1}), \dots, \mathbb{E}(\mathbf{A}_m)]). \end{aligned}$$

Taking the minimum with respect to $\omega \in \Omega$, we obtain

$$(7.3) \quad \begin{aligned} \min_{\omega \in \Omega} \min_{\omega' \in \Omega} \rho_j(\mu[\mathbf{A}_1(\omega), \dots, \mathbf{A}_{i-1}(\omega), \mathbf{A}_i(\omega'), \mathbb{E}(\mathbf{A}_{i+1}), \dots, \mathbb{E}(\mathbf{A}_m)]) \\ \min_{\omega \in \Omega} \rho_j(\mu[\mathbf{A}_1(\omega), \dots, \mathbf{A}_{i-1}(\omega), \mathbb{E}(\mathbf{A}_i), \mathbb{E}(\mathbf{A}_{i+1}), \dots, \mathbb{E}(\mathbf{A}_m)]). \end{aligned}$$

Suppose the minimum in the left hand side is attained in $\omega = \omega_0, \omega' = \omega'_0$. By independence of the random matrices \mathbf{A}_i , we have

$$\begin{aligned} \mathbf{p}(\{\sigma \in \Omega : \mathbf{A}_1(\sigma) = \mathbf{A}_1(\omega_0), \dots, \mathbf{A}_{i-1}(\sigma) = \mathbf{A}_{i-1}(\omega_0), \mathbf{A}_i(\sigma) = \mathbf{A}_i(\omega'_0)\}) \\ \mathbf{p}(\{\sigma \in \Omega : \mathbf{A}_1(\sigma) = \mathbf{A}_1(\omega_0), \dots, \mathbf{A}_{i-1}(\sigma) = \mathbf{A}_{i-1}(\omega_0)\}) \mathbf{p}(\{\sigma \in \Omega : \mathbf{A}_i(\sigma) = \mathbf{A}_i(\omega'_0)\}) > 0. \end{aligned}$$

Taking $\sigma_0 \in \Omega$ in the set in the left hand side, we obtain

$$\begin{aligned} \min_{\sigma \in \Omega} \rho_j(\mu[\mathbf{A}_1(\sigma), \dots, \mathbf{A}_{i-1}(\sigma), \mathbf{A}_i(\sigma), \mathbb{E}(\mathbf{A}_{i+1}), \dots, \mathbb{E}(\mathbf{A}_m)]) \\ \leq \rho_j(\mu[\mathbf{A}_1(\sigma_0), \dots, \mathbf{A}_{i-1}(\sigma_0), \mathbf{A}_i(\sigma_0), \mathbb{E}(\mathbf{A}_{i+1}), \dots, \mathbb{E}(\mathbf{A}_m)]) \\ = \rho_j(\mu[\mathbf{A}_1(\omega_0), \dots, \mathbf{A}_{i-1}(\omega_0), \mathbf{A}_i(\omega'_0), \mathbb{E}(\mathbf{A}_{i+1}), \dots, \mathbb{E}(\mathbf{A}_m)]) \\ = \min_{\omega \in \Omega} \min_{\omega' \in \Omega} \rho_j(\mu[\mathbf{A}_1(\omega), \dots, \mathbf{A}_{i-1}(\omega), \mathbf{A}_i(\omega'), \mathbb{E}(\mathbf{A}_{i+1}), \dots, \mathbb{E}(\mathbf{A}_m)]). \end{aligned}$$

This inequality, together with (7.3), implies (7.2), finishing thus the proof of the theorem. \square

Remark 7.3. The point of Theorem 7.2 is that the middle term might be easier to compute or to estimate. But, since the matrices $\mathbb{E}(\mathbf{A}_1), \dots, \mathbb{E}(\mathbf{A}_m)$ are *not* of rank one, Theorem 6.6 does not apply, and $\mu[\mathbb{E}(\mathbf{A}_1), \dots, \mathbb{E}(\mathbf{A}_m)]$ is not a characteristic polynomial. However, Theorem 7.2 tells us that its roots can be used to estimate the eigenvalues of $\mathbf{A}(\omega)$ for at least *some* value of ω .

Corollary 7.4. *Let $\mathbf{A}_1(\omega), \dots, \mathbf{A}_m(\omega)$ be independent rank one positive random matrices in $M_d(\mathbb{C})$, and $\mathbf{A} = \mathbf{A}_1 + \dots + \mathbf{A}_m$. Suppose $\mathbb{E}(\mathbf{A}) = I_d$ and $\mathbb{E}(\text{Tr } \mathbf{A}_i) \leq \epsilon$ for some $\epsilon > 0$. Then*

$$\min_{\omega \in \Omega} \|\mathbf{A}(\omega)\| \leq (1 + \sqrt{\epsilon})^2.$$

Proof. Since $\text{Tr}(\mathbb{E}(\mathbf{A}_i)) = \mathbb{E}(\text{Tr } \mathbf{A}_i) \leq \epsilon$, the matrices $\mathbb{E}(\mathbf{A}_1), \dots, \mathbb{E}(\mathbf{A}_m)$ satisfy the hypotheses of Theorem 6.4, all roots of $\mu[\mathbb{E}(\mathbf{A}_1), \dots, \mathbb{E}(\mathbf{A}_m)]$ are smaller than $(1 + \sqrt{\epsilon})^2$. By Theorem 7.2 we obtain, in particular,

$$\min_{\omega \in \Omega} \|\mathbf{A}(\omega)\| = \min_{\omega \in \Omega} \rho_1(p_{\mathbf{A}(\omega)}) \leq \rho_1(\mu[\mathbb{E}(\mathbf{A}_1), \dots, \mathbb{E}(\mathbf{A}_m)]) \leq (1 + \sqrt{\epsilon})^2. \quad \square$$

7.2. Probability and partitions. The last theorem of this section gets us closer to the paving conjecture. It is here that we make the connection between the probability space and the partitions. Let us first note that, similarly to Remark 6.7, one can see that the independence condition is not affected by a change of basis. So in Theorem 7.2 and in Corollary 7.4 we may assume that \mathbf{A}_i take values in $\mathcal{L}(V)$ for some finite dimensional vector space V . This observation will be used in the proof of the next theorem.

Theorem 7.5. *Suppose $A_1, \dots, A_m \in M_d(\mathbb{C})$ are positive rank one matrices, such that $\sum_{i=1}^m A_i = I_d$ and $\|A_i\| \leq C$ for all $i = 1, \dots, m$. Then for every positive integer r there exists a partition S_1, \dots, S_r of $\{1, \dots, m\}$, such that*

$$\left\| \sum_{i \in S_j} A_i \right\| \leq \left(\frac{1}{\sqrt{r}} + \sqrt{C} \right)^2$$

for any $j = 1, \dots, r$.

Proof. Since the purpose is to find a partition with certain properties, we will take as a random space Ω precisely the space of all partitions of $\{1, \dots, m\}$ in r sets, with uniform probability \mathbf{p} . Such a partition is determined by an element $\omega = (\omega_1, \dots, \omega_m)$, where $\omega_j \in \{1, \dots, r\}$, and $S_j = \{k : \omega_k = j\}$; so $\Omega = \{1, \dots, r\}^m$. Also, the different coordinates, that is the maps $\omega \mapsto \omega_i$, are independent scalar random variables on Ω .

We consider the space $V := \mathbb{C}^d \oplus \dots \oplus \mathbb{C}^d$ and define the random matrices \mathbf{A}_i ($i = 1, \dots, m$) with values in $\mathcal{L}(V)$ by

$$(7.4) \quad \mathbf{A}_i(\omega) = 0 \oplus \dots \oplus r A_i \oplus \dots \oplus 0,$$

where $r A_i$ appears in position ω_i .

These are independent random matrices (since the coordinates ω_i are independent). If we fix $1 \leq j \leq r$, then $\omega_i = j$ with probability $1/r$, and so $r A_i$ appears in position j with probability $1/r$. Therefore

$$\mathbb{E}(\mathbf{A}_i) = \frac{1}{r} r A_i \oplus \dots \oplus \frac{1}{r} r A_i = A_i \oplus A_i \oplus \dots \oplus A_i.$$

If $\mathbf{A} = \mathbf{A}_1 + \cdots + \mathbf{A}_m$, then

$$\mathbb{E}(\mathbf{A}) = \sum_{i=1}^m \mathbb{E}(\mathbf{A}_i) = \sum_{i=1}^m (A_i \oplus A_i \oplus \cdots \oplus A_i) = I_V.$$

Since $\text{Tr } \mathbf{A}_i(\omega) = r \text{Tr } A_i$ for all i , we have

$$\mathbb{E}(\text{Tr } \mathbf{A}_i) = \mathbb{E}(r \text{Tr } A_i) = r \mathbb{E}(\|A_i\|) \leq rC.$$

Corollary 7.4 yields the existence of $\omega \in \Omega$ such that

$$\|\mathbf{A}(\omega)\| \leq (1 + \sqrt{rC})^2.$$

But, according to (7.4), we have

$$\mathbf{A}(\omega) = \left(r \sum_{\omega_i=1} A_i \right) \oplus \left(r \sum_{\omega_i=2} A_i \right) \oplus \cdots \oplus \left(r \sum_{\omega_i=r} A_i \right).$$

We define then $S_j = \{i : \omega_i = j\}$. It follows that $\|r \sum_{i \in S_j} A_i\| \leq (1 + \sqrt{rC})^2$ for all j , and dividing by r ends the proof of the theorem. \square

8. PROOF OF THE PAVING CONJECTURE

We may now proceed to the proof of the paving conjecture; from this point on all we need from the previous sections is Theorem 7.5. We first deal with orthogonal projections. For such operators the paving conjecture is trivially verified (exercise: if P is an orthogonal projection and $\text{diag } P = 0$, then $P = 0$). But we will prove a quantitative version of the paving conjecture, in which one does not assume zero diagonal.

Lemma 8.1. *Suppose $P \in M_m(\mathbb{C})$ is an orthogonal projection. For any $r \in \mathbb{N}$ there exists diagonal orthogonal projections $Q_1, \dots, Q_r \in M_m(\mathbb{C})$, with $\sum_{j=1}^r Q_j = I_m$, such that*

$$\|Q_j P Q_j\| \leq \left(\frac{1}{\sqrt{r}} + \sqrt{\|\text{diag } P\|} \right)^2$$

for all $j = 1, \dots, r$.

Proof. Denote by V the image of P , and $d = \dim V$. Let $(e_i)_{i=1}^m$ a basis in \mathbb{C}^m , and define on V the rank one positive operators A_i by $A_i(v) = \langle v, P(e_i) \rangle P(e_i)$. We have

$$(8.1) \quad \|A_i\| \leq \|P(e_i)\|^2 = \langle P(e_i), e_i \rangle \leq \|\text{diag } P\|,$$

and, for $v \in V$,

$$(8.2) \quad \langle A_i v, v \rangle = \langle v, P(e_i) \rangle \langle P(e_i), v \rangle = |\langle v, P e_i \rangle|^2 = |\langle v, e_i \rangle|^2.$$

Consequently,

$$\left\langle \sum_{i=1}^m A_i v, v \right\rangle = \sum_{i=1}^m \langle A_i v, v \rangle = \sum_{i=1}^m |\langle v, e_i \rangle|^2 = \|v\|^2,$$

whence

$$(8.3) \quad \sum_{i=1}^r A_i = I_V.$$

From (8.1) and (8.3) it follows that A_i satisfy the hypotheses of Theorem 7.5, with $C = \|\text{diag } P\|_\infty$. There exists therefore a partition S_1, \dots, S_r of $\{1, \dots, m\}$, such that

$$\left\| \sum_{i \in S_j} A_i \right\| \leq \left(\frac{1}{\sqrt{r}} + \sqrt{\|\text{diag } P\|_\infty} \right)^2$$

for any $j = 1, \dots, r$.

Define then $Q_j \in M_m(\mathbb{C})$ to be the diagonal orthogonal projection on the span of $\{e_i : i \in S_j\}$. Then

$$\|Q_j P Q_j\| = \|Q_j P (Q_j P)^*\| = \|Q_j P\|^2 = \|Q_j V\|^2.$$

But, if $v \in V$, then, applying (8.2),

$$\|Q_j v\|^2 = \sum_{i \in S_j} |\langle v, e_i \rangle|^2 = \sum_{i \in S_j} \langle A_i v, v \rangle = \langle \left(\sum_{i \in S_j} A_i \right) v, v \rangle \leq \left\| \sum_{i \in S_j} A_i \right\| \cdot \|v\|^2.$$

So

$$\|Q_j P Q_j\| = \|Q_j V\|^2 \leq \left\| \sum_{i \in S_j} A_i \right\| \leq \left(\frac{1}{\sqrt{r}} + \sqrt{\|\text{diag } P\|_\infty} \right)^2,$$

and the lemma is proved. \square

Theorem 8.2 (The paving conjecture). *For any $\epsilon > 0$ there exists $r \in \mathbb{N}$ such that, for any $m \in \mathbb{N}$ and $T \in M_m(\mathbb{C})$ with $\text{diag } T = 0$ there exist diagonal orthogonal projections $Q_1, \dots, Q_r \in M_m(\mathbb{C})$, with $\sum_{j=1}^r Q_j = I_m$, such that*

$$\|Q_j T Q_j\| \leq \epsilon \|T\|$$

for all $j = 1, \dots, r$.

Proof. Suppose first that $T = T^*$ and $\|T\| \leq 1$. The $2m \times 2m$ matrix

$$P = \begin{pmatrix} \frac{I_m + T}{2} & \frac{1}{2}(I_m - T^2)^{1/2} \\ \frac{1}{2}(I_m - T^2)^{1/2} & \frac{I_m - T}{2} \end{pmatrix}$$

is an orthogonal projection and $\text{diag } P = \left(\frac{1}{2}, \dots, \frac{1}{2}\right)$. Choose r large enough to have $2 \left(\frac{1}{\sqrt{r}} + \frac{1}{\sqrt{2}}\right)^2 - 1 \leq \epsilon$. It follows from Lemma 8.1 that there exist diagonal projections $Q_1'', \dots, Q_r'' \in M_{2m}(\mathbb{C})$ with $\sum_{i=1}^r Q_i'' = I_{2d}$ and $\|Q_i'' P Q_i''\| \leq \left(\frac{1}{\sqrt{r}} + \frac{1}{\sqrt{2}}\right)^2$ for all $i = 1, \dots, r$.

Let $Q_i'' = Q_i + Q_i'$ be the decomposition of Q_i'' in the diagonal projections corresponding to the first m and the last m vectors of the basis of \mathbb{C}^{2m} . So $\sum_{i=1}^r Q_i = \sum_{i=1}^r Q_i' = I_m$ and, for each $i = 1, \dots, m$,

$$(8.4) \quad \|Q_i(I + T)Q_i\| \leq 2 \left(\frac{1}{\sqrt{r}} + \frac{1}{\sqrt{2}} \right)^2, \quad \|Q_i'(I - T)Q_i'\| \leq 2 \left(\frac{1}{\sqrt{r}} + \frac{1}{\sqrt{2}} \right)^2.$$

The first inequality implies that $Q_i(I + T)Q_i \leq 2 \left(\frac{1}{\sqrt{r}} + \frac{1}{\sqrt{2}} \right)^2 Q_i$, so

$$(8.5) \quad -Q_i \leq Q_i T Q_i \leq \left[2 \left(\frac{1}{\sqrt{r}} + \frac{1}{\sqrt{2}} \right)^2 - 1 \right] Q_i \leq \epsilon Q_i$$

(the left inequality being obvious). Similarly, the second inequality in (8.4) yields

$$(8.6) \quad -\epsilon Q_i' \leq \left[1 - 2 \left(\frac{1}{\sqrt{r}} + \frac{1}{\sqrt{2}} \right)^2 \right] Q_i' \leq Q_i' T Q_i' \leq Q_i'.$$

If we define $Q_{ij} = Q_i Q_j'$ ($i, j = 1, \dots, r$), then $\sum_{i,j=1}^r Q_{ij} = I_m$, and it follows from (8.5) and (8.6) that

$$-\epsilon Q_{ij} \leq Q_{ij} T Q_{ij} \leq \epsilon Q_{ij},$$

or $Q_{ij} T Q_{ij} \leq \epsilon$. The theorem is thus proved for T a selfadjoint contraction, and it is immediate to extend it to arbitrary selfadjoint matrices.

If we take now an arbitrary $T \in M_m(\mathbb{C})$, with $\text{diag } T = 0$, we may write it as $T = A + iB$, with A, B selfadjoint, $\|A\|, \|B\| \leq \|T\|$, and $\text{diag } A = \text{diag } B = 0$. Applying the first step, one finds diagonal projections $Q_1', \dots, Q_r', Q_1'', \dots, Q_r'' \in M_m(\mathbb{C})$, with $\sum_{i=1}^r Q_i' = \sum_{i=1}^r Q_i'' = I_m$, $\|Q_i' A Q_i'\| \leq \frac{\epsilon}{2} \|T\|$ and $\|Q_i'' B Q_i''\| \leq \frac{\epsilon}{2} \|T\|$ for $i = 1, \dots, r$. If we define $Q_{ij} = Q_i' Q_j''$, then $\sum_{i,j=1}^r Q_{ij} = I_m$, and $\|Q_{ij} T Q_{ij}\| \leq \epsilon \|T\|$ for $i, j = 1, \dots, r$. \square

By writing carefully the estimates in the proof, one sees also that we may take r of order ϵ^{-4} .

9. FINAL REMARKS

1. As noted in Remark 2.6, there is a connection between the Kadison–Singer problem and quantum mechanics. We will give here a very perfunctory account. In the von Neumann picture of quantum mechanics, states (in the common sense) of a system correspond to states ϕ (in the C^* -algebra sense) of $B(\mathcal{H})$, while observables of the system correspond to selfadjoint operators $A \in B(\mathcal{H})$. The value of an observable in a state is precisely $\phi(A)$.

A maximal abelian C^* -algebra $\mathcal{A} \subset B(\mathcal{H})$ corresponds to a maximal set of mutually compatible observables. If the extension of any pure state on \mathcal{A} to a state on $B(\mathcal{H})$ is unique, then one can say that the given set of observables determines completely all other observables. This seems to have been assumed by Dirac implicitly.

Now, there are various maximal abelian subalgebras of $B(\mathcal{H})$, but the problem can essentially be reduced to two different basic types: continuous (that are essentially isomorphic to L^∞ acting as multiplication operators on L^2) and discrete (that are isomorphic to \mathcal{D} acting in ℓ^2). The main topic of the original paper [7] is to prove that extension of pure states is *not* unique in general for continuous subalgebras. They suspected that the same thing happens for the discrete case, but could not prove it, and so posed it as an open problem.

2. We have said in the introduction that there are many statements that had been shown to be equivalent to (KS), besides (PC) that we have used in an essential way. We have thus, among others:

- (1) Weaver’s conjectures in discrepancy theory. The original proof in [10] goes actually through one of these; the shortcut using (PC) is due to Tao [14].
- (2) Feichtinger’s conjecture in frame theory.
- (3) Bourgain–Tzafriri conjecture.

All these conjectures have in fact different forms, weaker or stronger variants, etc—a detailed account may be found in [4]. It is worth noting that up to 2013 most specialists believed that they are not true, and that a counterexample will eventually be found. So it was a surprise when all these statements were simultaneously shown true by [10].

3. The method used in [10] is even stronger than described above. Actually, its first application was to a completely different problem in graph theory: the existence of certain infinite families of so-called Ramanujan graphs [9] (see also [11] for an account).

4. The most tedious proof in the above notes is that of Lemma 5.5. The original argument in [10] is more elegant, but uses another result of Borcea and Brändén [3] that represents real stable polynomials in two variables as determinants of certain matrices—a kind of converse to Lemma 5.2. The direct argument we use appears in [14].

REFERENCES

- [1] J. Anderson: Extensions, restrictions and representations of states on C^* -algebras, *Trans. AMS* 249 (1979), 195–217.
- [2] J. Borcea, P. Brändén: Applications of stable polynomials to mixed determinants: Johnson’s conjectures, unimodality, and symmetrized Fischer products, *Duke Math. Journal* 143 (2008), 205–223.
- [3] J. Borcea, P. Brändén: Multivariate Pólya–Schur classification problems in the Weyl algebra, *Proc. Lond. Math. Soc.* (3) 101 (2010), 73–104.
- [4] P.G. Cassazza, M. Fickus, J.C. Tremain, E. Weber: The Kadison–Singer problem in mathematics and engineering: a detailed account, *Operator Theory, Operator Algebras, and Applications*, 299–355, *Contemp. Math.* 414, AMS, 2006.
- [5] P.A.M. Dirac: *The Principles of Quantum Mechanics*, Oxford University Press, 1958.
- [6] R.V. Kadison, J.R. Ringrose: *Fundamentals of the Theory of Operator Algebras*, Academic Press, 1983.
- [7] R.V. Kadison, I.M. Singer: Extensions of pure states, *American Jour. Math.* **81** (1959), 383–400.
- [8] T. Kato, *Perturbation Theory for Linear Operators*, Springer-Verlag, 1980.
- [9] A. Marcus, D.A. Spielman, N. Srivastava: Interlacing families I: Bipartite Ramanujan graphs of all degrees, arxiv:1304.4132.
- [10] A. Marcus, D.A. Spielman, N. Srivastava: Interlacing families II: Mixed characteristic polynomials and the Kadison–Singer problem, arxiv:1306.3969.
- [11] A. Marcus, D.A. Spielman, N. Srivastava: Ramanujan graphs and the solution to the Kadison–Singer Problem, arxiv:1408.4421v1, to appear in *Ann. of Math.*
- [12] M.A. Naimark: *Normed Algebras*, Wolters–Noordhoff, Groningen, 1972.
- [13] C. Procesi: The invariant theory of $n \times n$ matrices, *Adv. in Math.* 19 (1976), 306–381.
- [14] T. Tao: Real stable polynomials and the Kadison–Singer problem, <https://terrytao.wordpress.com/tag/kadison-singer-problem/>.
- [15] A. Valette: Le problème de Kadison–Singer, arxiv:1409.5898v.